Allan Carey
Program Manager
Information Security Services

Business Continuity and Disaster Recovery:
Critical Measures for Business Survival

IDC
Analyze the Future

Agenda

- September 11th Effect
- Defining BC and DR
- The Importance of Security
- Conclusions

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

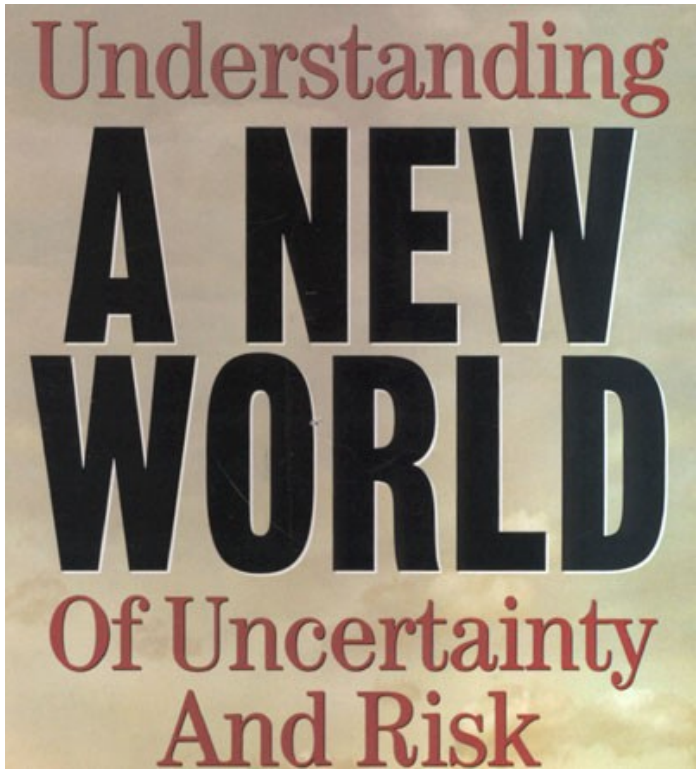
Pre-September 11

- Economy enters into recession
- Some companies have business continuity plans, on the shelf
- Plans were insufficient
- Initiatives driven with a “bottoms up” approach

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

The September 11th Effect



IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

The September 11th Effect

- Terrorist attacks cause more than $50 billion in infrastructure damage
- Dramatically raised awareness
  - Physical and cyber security
- Business leaders closely examining internal security, continuity, and recovery plans
  - 90% of CEOs have reviewed DR plans*
- Many discover inadequate investments

*Source: AP or Reuters

* Source: Booz Allen Hamilton survey, Jan. 23, 2002

IDC Analyze the Future

Copyright 2002 IDC. All rights reserved.

Post-September 11

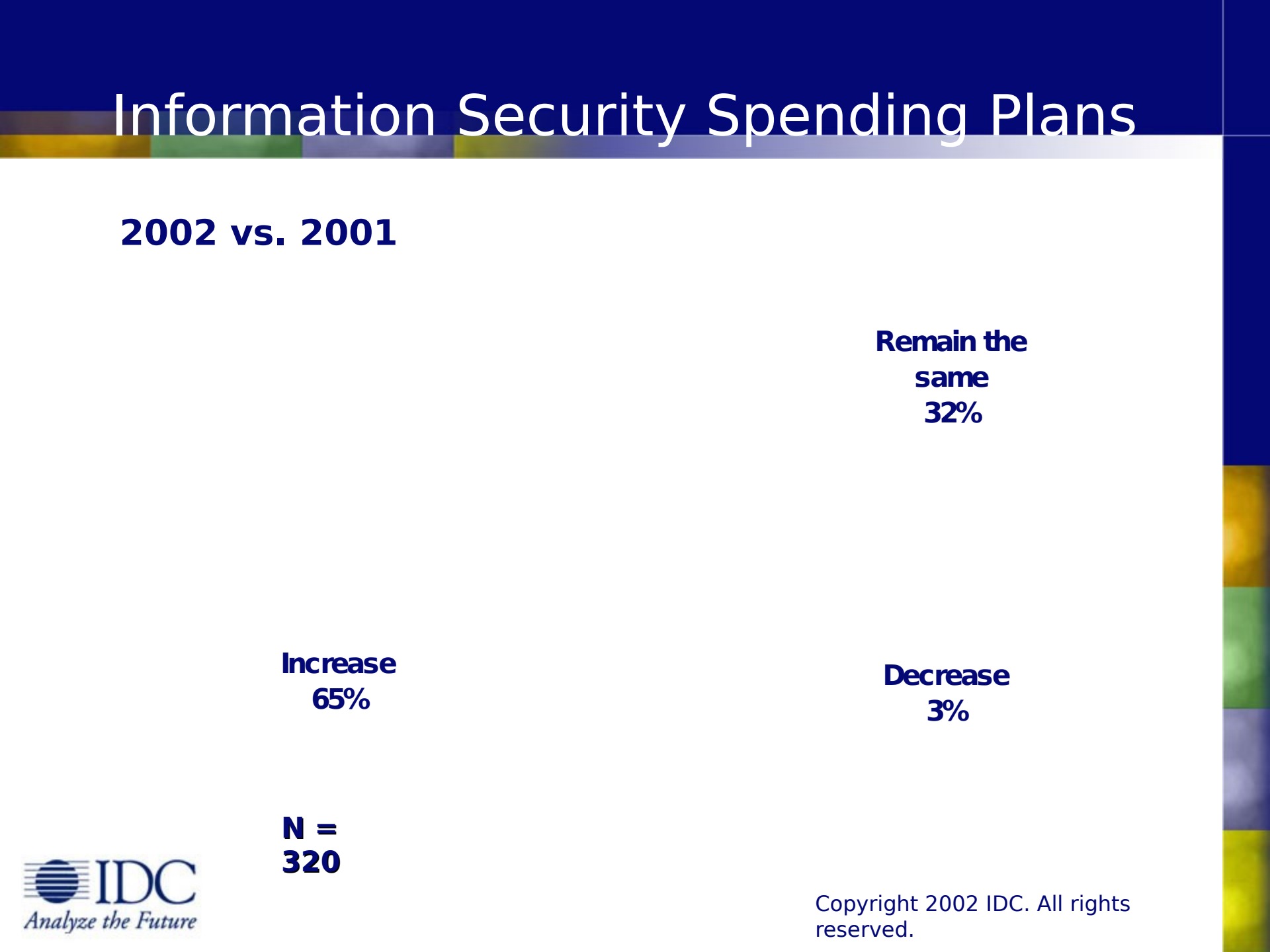
- Economic recession exacerbated
- BCP services gaining momentum in the marketplace
- Security services firms continue portfolio buildout to include BCP and incident readiness
- Development for National Strategy to Secure Cyberspace underway

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

Information Security Spending Plans

2002 vs. 2001



IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

Agenda

- September 11th Effect
- Defining BC and DR
- The Importance of Security
- Conclusions

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

Types of Contingency Plans

Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed only in the context of supporting business process
Business Recovery (or Resumption) Plan (BRP)	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused
Continuity of Operations Plan	Establish procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days	Addresses subset of an organization's missions deemed critical; not IT-focused
Continuity of Support Plan	Establish procedures and capabilities for recovering a major application or general support system	Similar to IT contingency plan; addresses IT system disruption; not business process focused
Disaster Recovery Plan (DRP)	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Incident Response Plan	Define strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
Occupant Emergency Plan	Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not business- or IT-focused

http://csrc.nist.gov/publications/drafts/ITcontingency-planning-guideline.pdf

IDC Analyze the Future

Copyright 2002 IDC. All rights reserved.

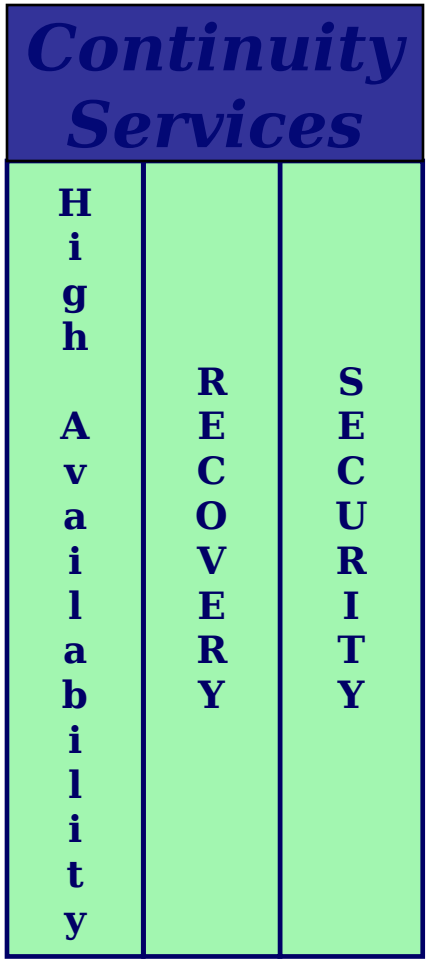
What is Business Continuity?

Business continuity describes the processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster. Business continuance planning seeks to prevent interruption of mission-critical services, and to reestablish full functioning as swiftly and smoothly as possible.

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

What is Business Continuity?



- Simply put, it's the means of keeping an organization up and running 24 x 7 despite any expected or unexpected disruption.
- May involve highly available, "always on" infrastructures that make traditional recovery obsolete
- May involve traditional disaster recovery services, I.e. hot/cold site, data backup, mobile recovery, contingency planning (reactive approach) OR
- May involve security services (proactive approach)

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

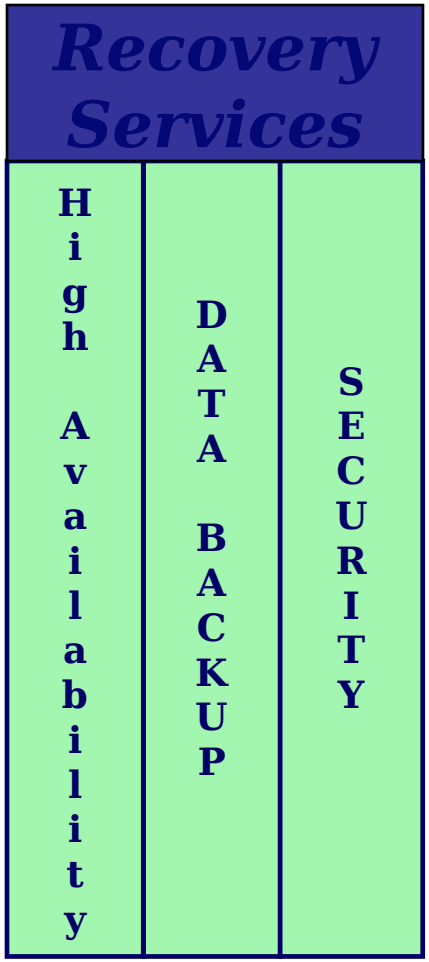
What is Disaster Recovery?

Disaster recovery describes how an organization is to deal with potential disasters. A disaster recovery plan (DRP) consists of the precautions taken so that the effects of a disaster will be minimized, and the organization will be able to either maintain or quickly resume mission-critical functions.

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

What is Disaster Recovery?



- It's a crucial component of business continuity that addresses more of the IT functions necessary to resume business operations due to an expected or unexpected disruption.
- May involve highly available, redundant infrastructures i.e., hot/cold site, bandwidth capacity, scalable network
- May involve traditional data backup services, i.e., data replication, offsite data backup storage, mobile recovery, (reactive approach)
- May involve security services (proactive approach)

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

7-Step Process

- Review/refresh or develop security, disaster recovery, and BC plans
- Develop contingency planning policy
- Conduct business impact analysis (BIA)
- Identify preventative controls
- Develop recovery strategies
- Develop contingency plan
- Plan testing, training and simulations
- Maintain the plan

Source: NIST

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

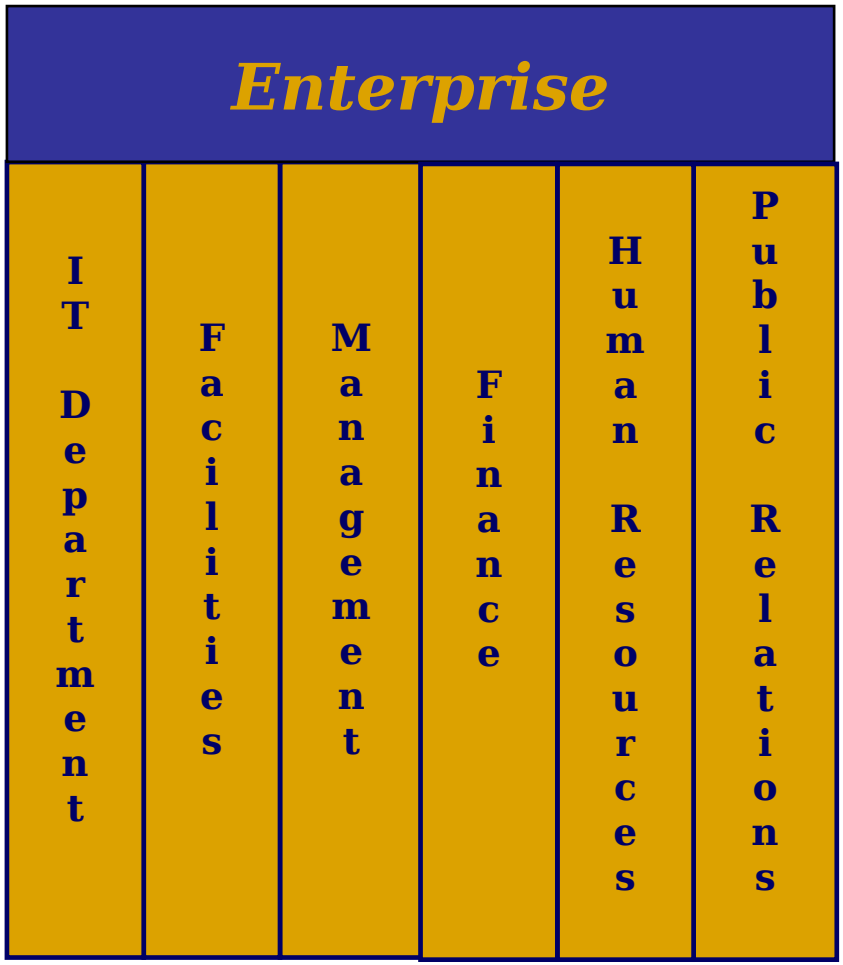
Agenda

- September 11th Effect
- Defining BC and DR
- The Importance of Security
- Conclusions

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

Silos of Security



- Security often resides in many different departments
- Lack of communication and coordination
- Delayed response
- Prolonged recovery cycle

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

Post-911 Assessment

- Not just a Government problem
- US corporations represent the most vulnerable
- Current Government spending mainly focused on physical security (i.e.,gates, guns, guards, & dogs)
- No significant Government spending on IT security until late 2003/2004
- Convergence of physical and IT security in 2005 and 2006

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

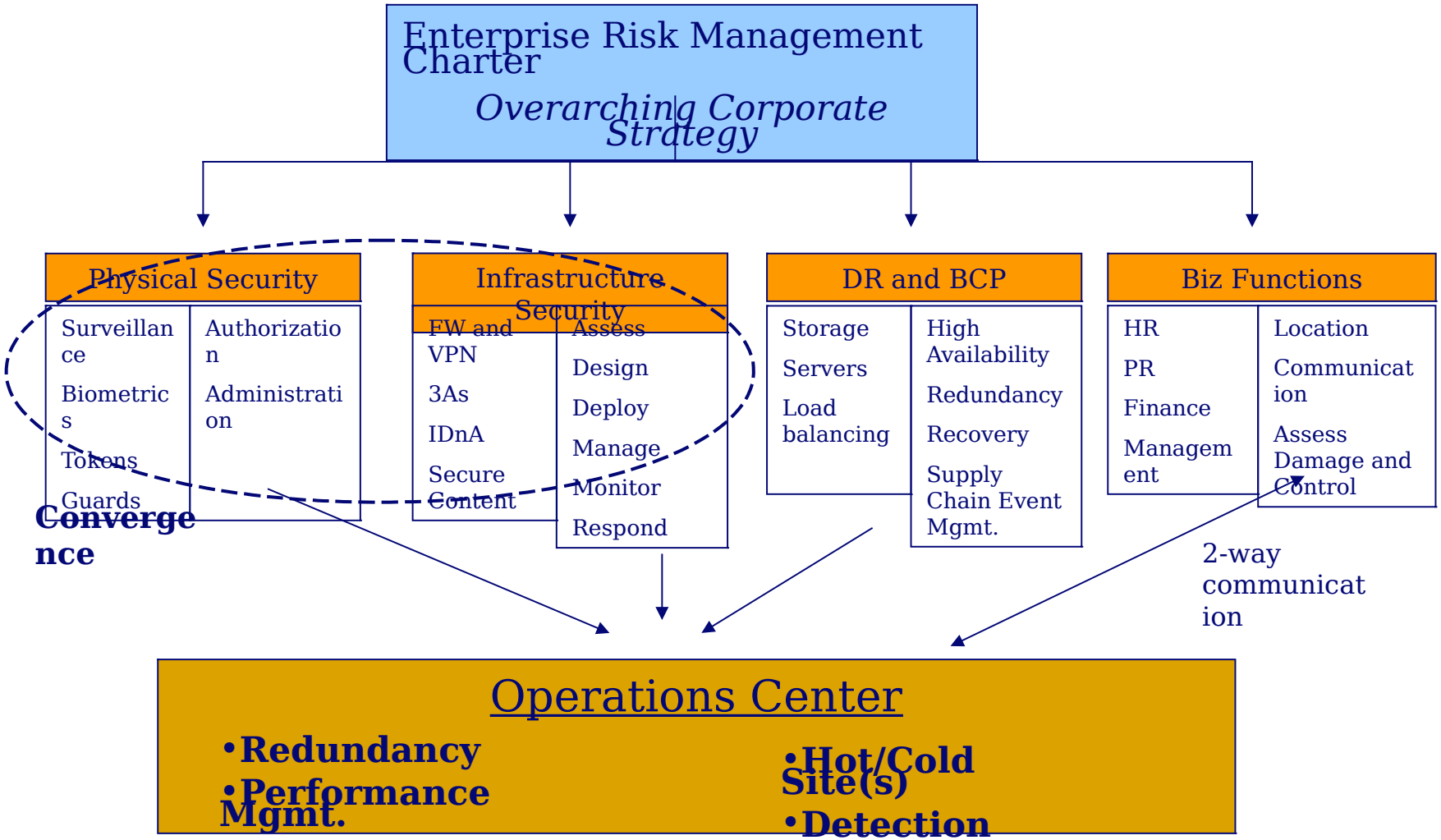
The Need for Security and BC Planning

- Enterprise-wide security and BC strategy
- More communication and coordination across business units
- Improved response and better accountability

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

Enterprise Risk Management



Copyright 2002 IDC. All rights reserved.

Agenda

- September 11th Effect
- Defining BC and DR
- The Importance of Security
- Conclusions

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

Conclusions

- Physical and IT security will become more tightly integrated
- BCP must encompass all aspects of an organization
- Security is a crucial component to BC and disaster prevention
- Proper identification, planning, and implementation will ensure not only success, but *business survival*

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

Questions?

Please email me at

acarey@idc.com

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.

IDC
Analyze the Future

Copyright 2002 IDC. All rights reserved.